RSA Conference2019
Asia Pacific & Japan
Singapore | 16–18 July | Marina Bay Sands

SESSION ID: SDS-R04

Distributed forensic collection and analysis

Dr Michael Cohen
Digital Paleontologist
Velocidex Enterprises

Nick Klein
Director, Velocidex Enterprises
Director, Klein & Co. Computer Forensics
SANS DFIR Certified Instructor

Who are we?

Dr Michael Cohen

- Experienced digital forensic software developer
- Developer of foundation forensic tools including Volatility and Rekall
- Former lead developer of Grr Rapid Response at Google Inc.

Nick Klein

- Director of Klein & Co. digital forensic and cyber response team
- SANS DFIR Certified Instructor

What's the challenge?

Deep visibility of endpoints is a game changer for digital forensic investigations, threat hunting and cyber breach response.

Many endpoint monitoring products now exist, but there are few powerful tools to **truly interrogate and collect historic evidence** from across a network.

For example, an EDR tool may show network connections, but can it also interrogate the Internet history of all users?

We're building Velociraptor to address these limitations.

Why Velociraptor?

Velociraptor is a unique DFIR tool, giving *you* power and flexibility through the Velociraptor Query Language (VQL)

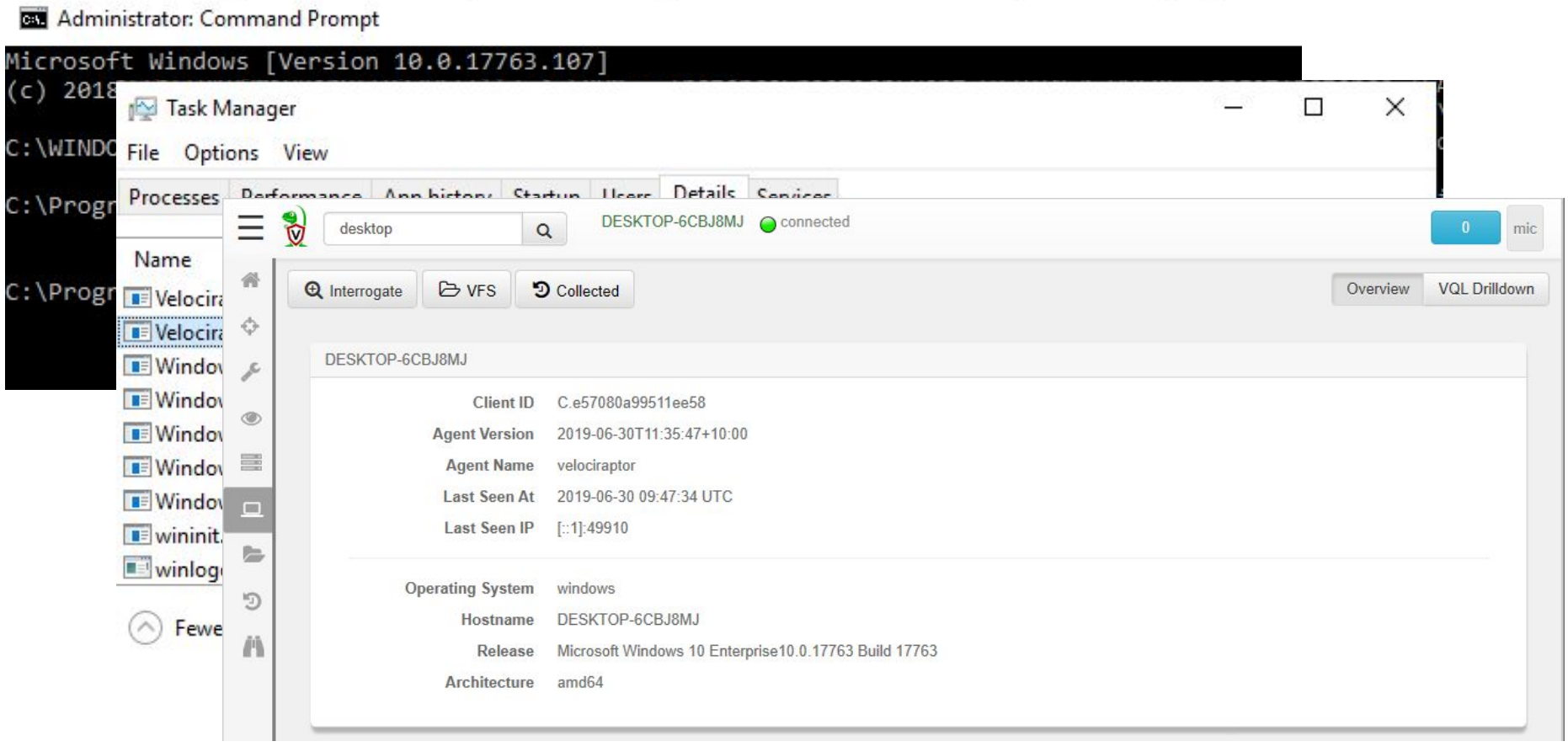
VQL is used for everything:

- Collecting information from endpoints
- Controlling monitoring and response
- Controlling and managing the server

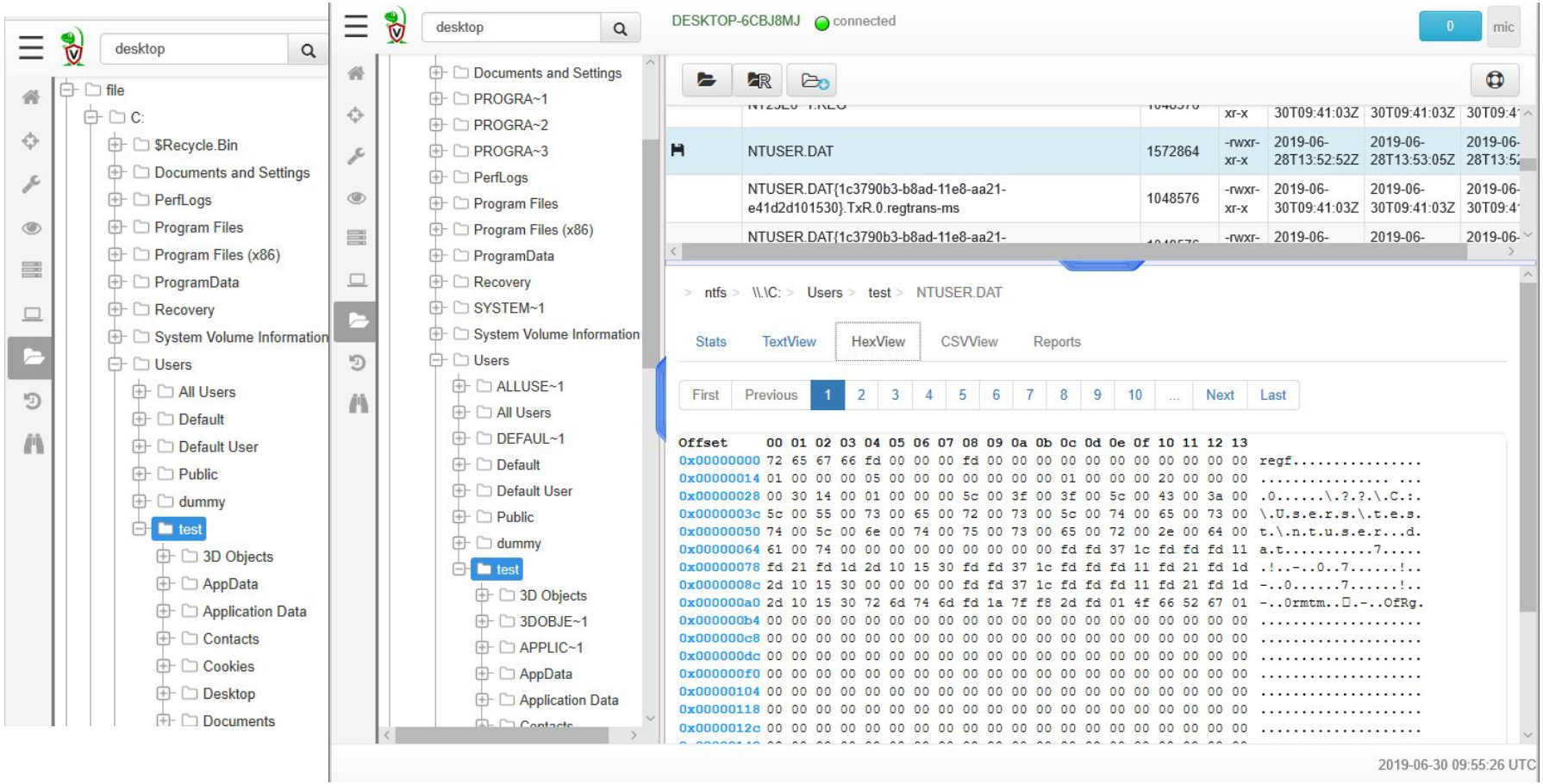
Easy server setup

```
C:\Program Files\Velocira
?
Welcome to the Velociraptor
------------------------

I will be creating a new
begin by identifying what

 Self Signed SSL
Generating keys please wa
? Enter the frontend port
? What is the public DNS
? Path to the datastore d
? Path to the logs direct
? Where should i write th
? Where should i write th
? GUI Username or email a
? GUI Username or email a

C:\Program Files\Velocira
```

Deploying clients



Browse remote computers



Use Velociraptor artifacts to automate everything

We can collect information about *many* things in DFIR cases:

- Registry keys, files, WMI queries, Sqlite databases …

But we often need to answer specific questions:

- What program did the attacker run?
- What files were downloaded?
- What DNS lookups occurred?
- Did a particular file exist on an endpoint?

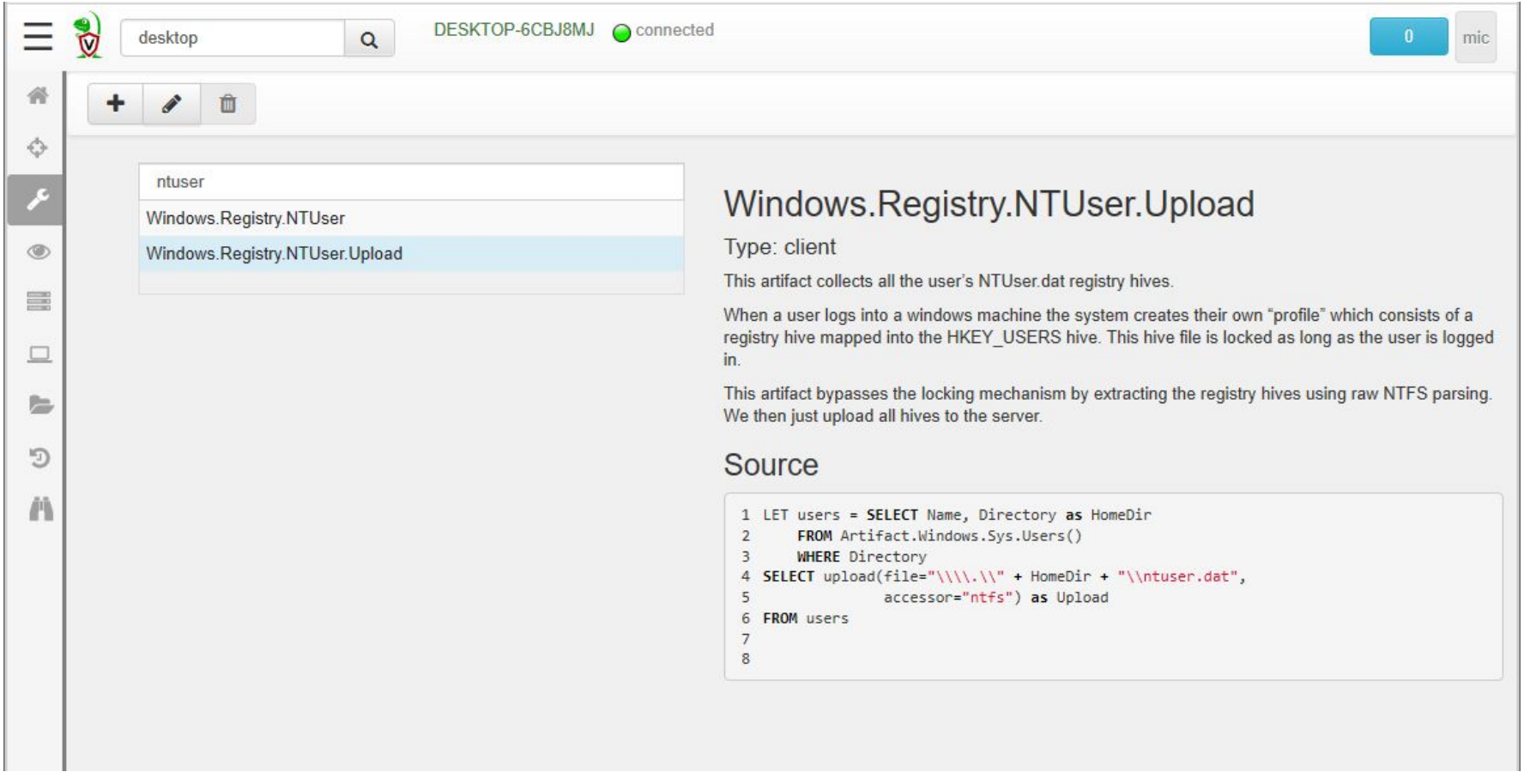
Use expert knowledge to find the evidence

A key objective of Velociraptor is encapsulating DFIR knowledge into the tool:

- We have high level questions to answer
- We know where to look for evidence of user / system activities

We build artifacts to collect and analyze the evidence in order to answer our investigative questions.

Single endpoint collection



Hunting is the collection of artifacts across the network

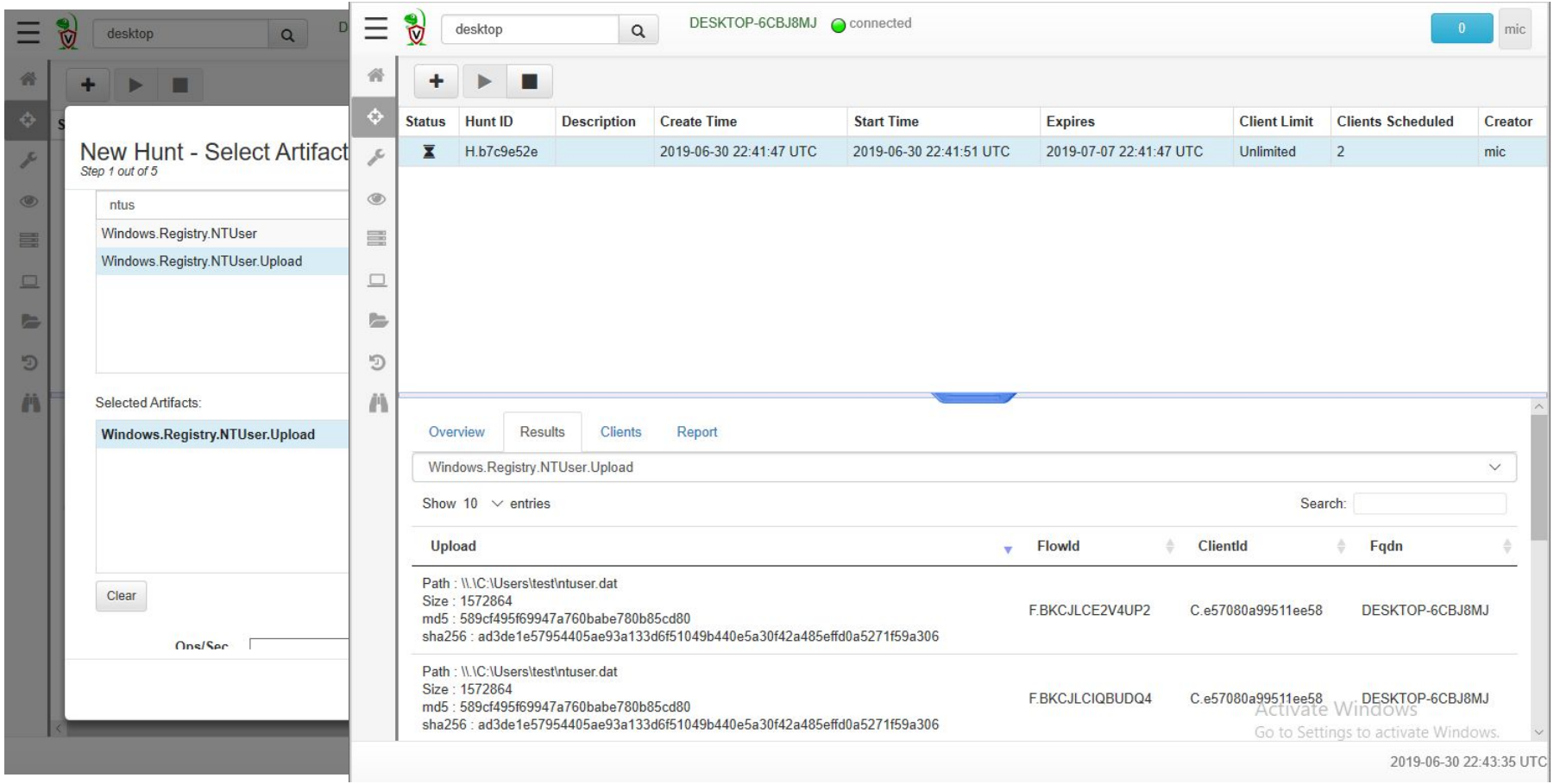
Any artifact that can be collected on a single computer, can be hunted across the network

A hunt can cover a group of clients, or the whole network

A hunt will continue running until it expires, or is stopped

As new machines appear, they automatically join in the hunt

Network-wide hunts



Scenario: Finding files across endpoints

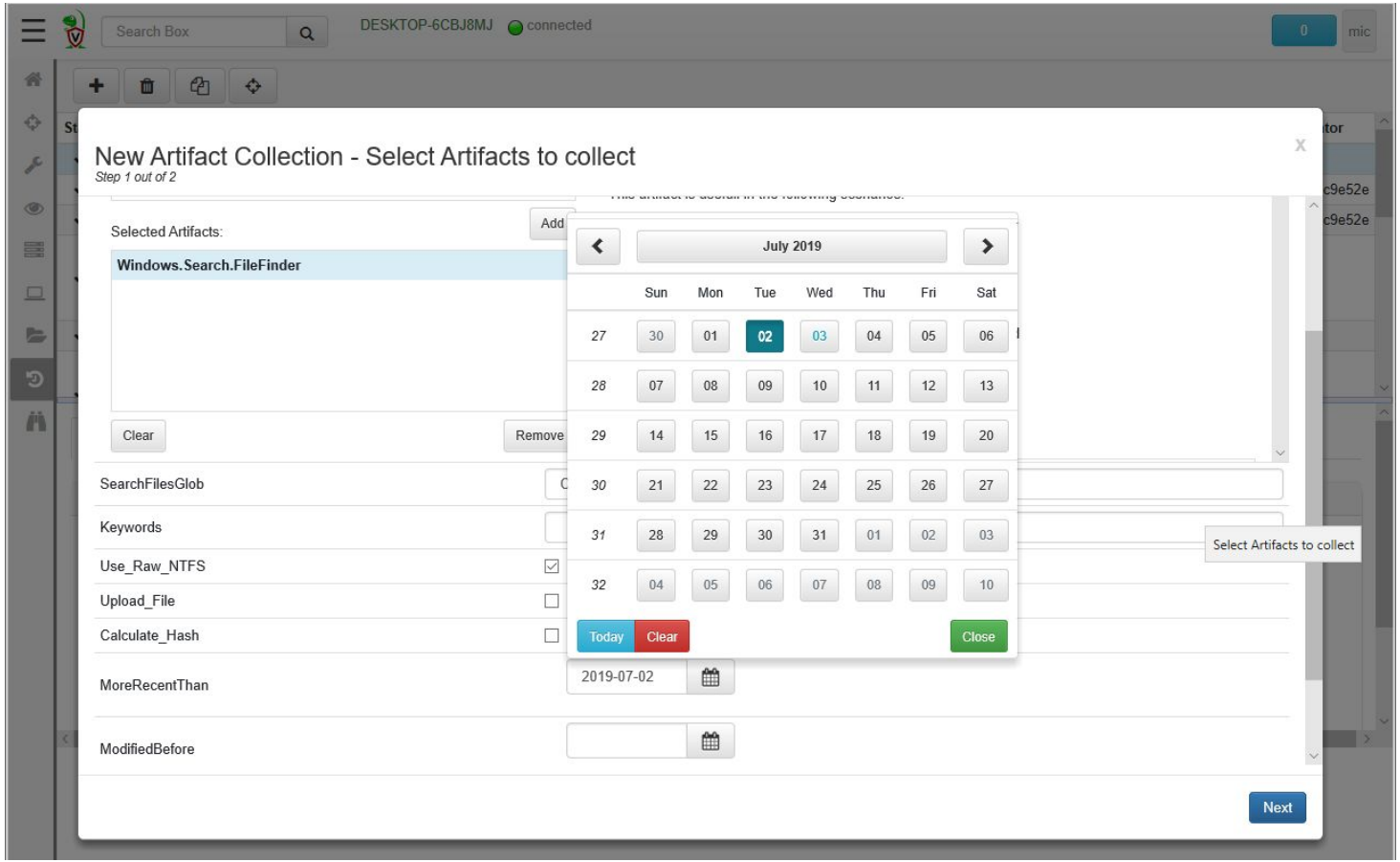
Searching for files is a fundamental capability.

Velociraptor provides a powerful **File Finder** artifact for this.

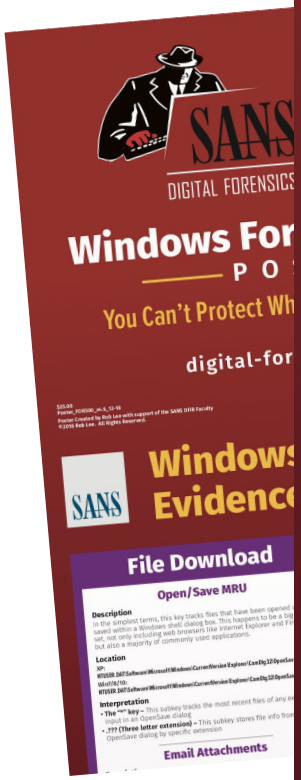
- Use wildcards to ‘glob’ over directories
- Use Yara to search the contents of files for keywords
- Filter by modified or created dates
- Upload matching files to the server, for further analysis.

The **Windows.Search.FileFinder** is a great start for many custom artifacts - just copy/paste and pre-populate with the right defaults.

Scenario: Finding files across endpoints



Scenario: Hunt for evidence of program execution



Program Execution

UserAssist

Description

GUI-based programs launched from the desktop are tracked in the launcher on a Windows System.

Location

NTUSER.DAT HIVE:
NTUSER.DAT\Software\Microsoft\Windows\Currentversion\Explorer\UserAssist\{GUID}\Count

Interpretation

All values are ROT-13 Encoded
- GUID for XP
  - 75048700 Active Desktop
- GUID for Win7/8/10
  - CEBFF5CD Executable File Execution
  - F4E57C4B Shortcut File Execution

Windows 10 Timeline

Description

Win10 records recently used applications and files in a "timeline" accessible via the "WIN+TAB" key. The data is recorded in a SQLite database.

Location

C:\Users\<profile>\AppData\Local\ConnectedDevicesPlatform\L.<profile>\ActivitiesCache.db

Interpretation
- Application execution
- Focus count per application

RecentApps

Description

GUI Program execution launched on the Win10 system is tracked in the RecentApps key

Location

Win10:
NTUSER.DAT\Software\Microsoft\Windows\Current Version\Search\RecentApps

Interpretation

Each GUID key points to a recent application.
AppID = Name of Application
LastAccessTime = Last execution time in UTC
LaunchCount = Number of times executed

Shimcache

Description
- Windows Application Compatibility Database is used by Windows to identify possible application compatibility challenges with executables.
- Tracks the executables file name, file size, last modified time, and in Windows XP the last update time

Location

XP:
SYSTEM\CurrentControlSet\Control\SessionManager\AppCompatibility
Win7/8/10:
SYSTEM\CurrentControlSet\Control\Session Manager\AppCompatCache

Interpretation

Any executable run on the Windows system could be found in this key. You can use this key to identify systems that specific malware was executed on. In addition, based on the interpretation of the time-based data you might be able to determine the last time of execution or activity on the system.
- Windows XP contains at most 96 entries
  - LastUpdateTime is updated when the files are executed
- Windows 7 contains at most 1,024 entries
  - LastUpdateTime does not exist on Win7 systems

Jump Lists

Description
- The Windows 7 task bar (Jump List) is engineered to allow users to "jump" or access items they have frequently or recently used quickly and easily. This functionality cannot only include recent media files; it must also include recent tasks.
- The data stored in the AutomaticDestinations folder will each have a unique file prepended with the AppID of the associated application.

Location

Win7/8/10:
C:\%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations

Interpretation
- First time of execution of application.
  - Creation Time = First time item added to the AppID file.
- Last time of execution of application w/file open.
  - Modification Time = Last time item added to the AppID file.
- List of Jump List IDs ->
  http://www.forensicswiki.org/wiki/List_of_Jump_List_IDs

Amcache.hve

Description

ProgramDataUpdater (a task associated with the Application Experience Service) uses the registry file Amcache.hve to store data during process creation

Location

Win7/8/10:
C:\Windows\AppCompat\Programs\Amcache.hve

Interpretation
- Amcache.hve – Keys = **Amcache.hve\Root\File\{Volume GUID}\######**
- Entry for every executable run, full path information, File's $StandardInfo Last Modification Time, and Disk volume the executable was run from
- First Run Time = Last Modification Time of Key
- SHA1 hash of executable also contained in the key

System Resource Usage Monitor (SRUM)

Description

Records 30 to 60 days of historical system performance. Applications run, user account responsible for each, and application and bytes sent/received per application per hour.

Location

SOFTWARE\Microsoft\WindowsNT\CurrentVersion\SRUM\Extensions\{d10ca2fe-6fcf-4f6d-848e-b2e99266fa89} = Application Resource Usage Provider C:\Windows\System32\SRU

Interpretation

Use tool such as **srum_dump.exe** to cross correlate the data between the registry keys and the SRUM ESE Database.

BAM/DAM

Description

Windows Background Activity Moderator (BAM)

Location

Win10:
SYSTEM\CurrentControlSet\Services\bam\UserSettings\{SID}
SYSTEM\CurrentControlSet\Services\dam\UserSettings\{SID}

Investigative Notes

Provides full path of the executable file that was run on the system and last execution date/time

Last-Visited MRU

Description

Tracks the specific executable used by an application to open the files documented in the OpenSaveMRU key. In addition, each value also tracks the directory location for the last file that was accessed by that application.
Example: Notepad.exe was last run using the **C:\%USERPROFILE%\Desktop** folder

Location

XP:
NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedMRU
Win7/8/10:
NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedPidlMRU

Interpretation

Tracks the application executables used to open files in OpenSaveMRU and the last file path used.

Prefetch

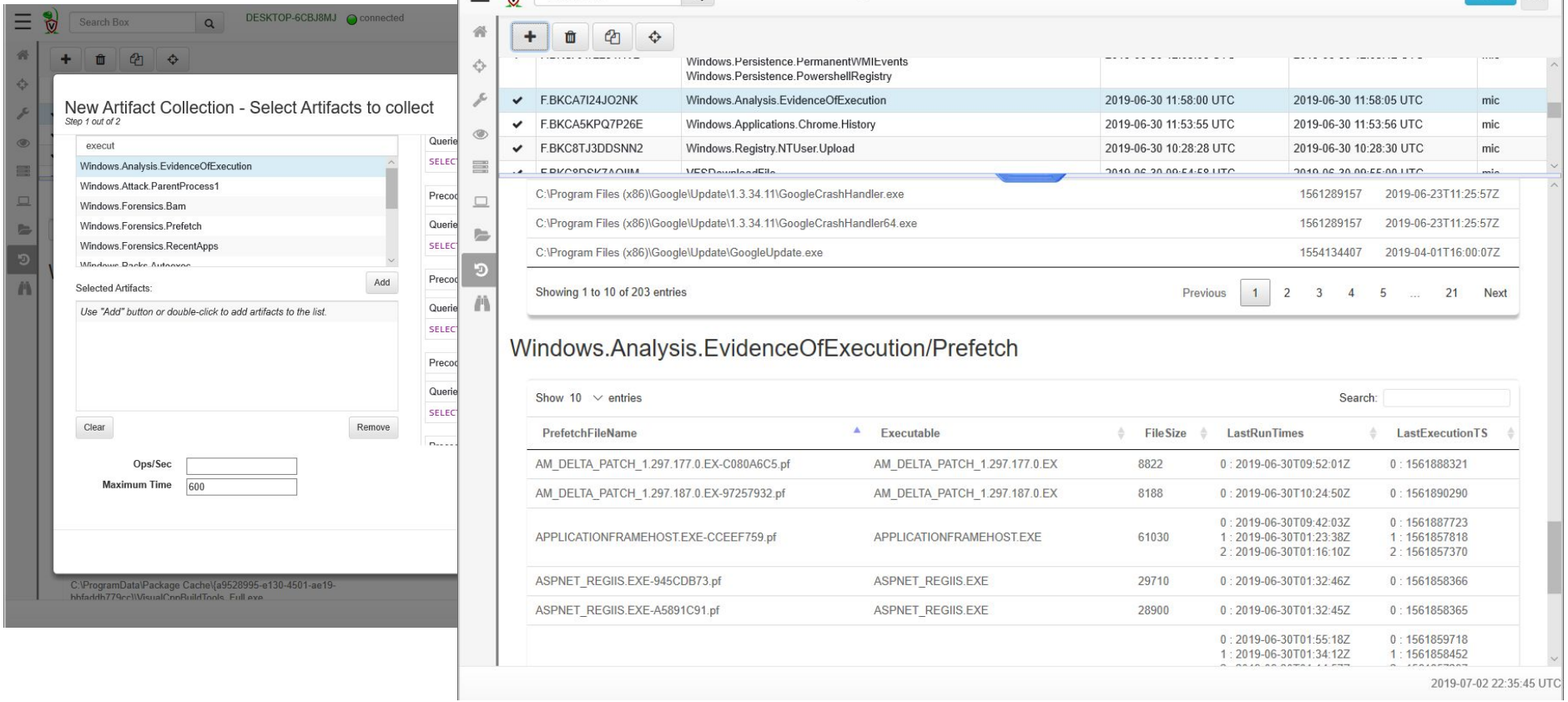
Description
- Increases performance of a system by pre-loading code pages of commonly used applications. Cache Manager monitors all files and directories referenced for each application or process and maps them into a .pf file. Utilized to know an application was executed on a system.
- Limited to 128 files on XP and Win7
- Limited to 1024 files on Win8
- (exename)-(hash).pf

Location

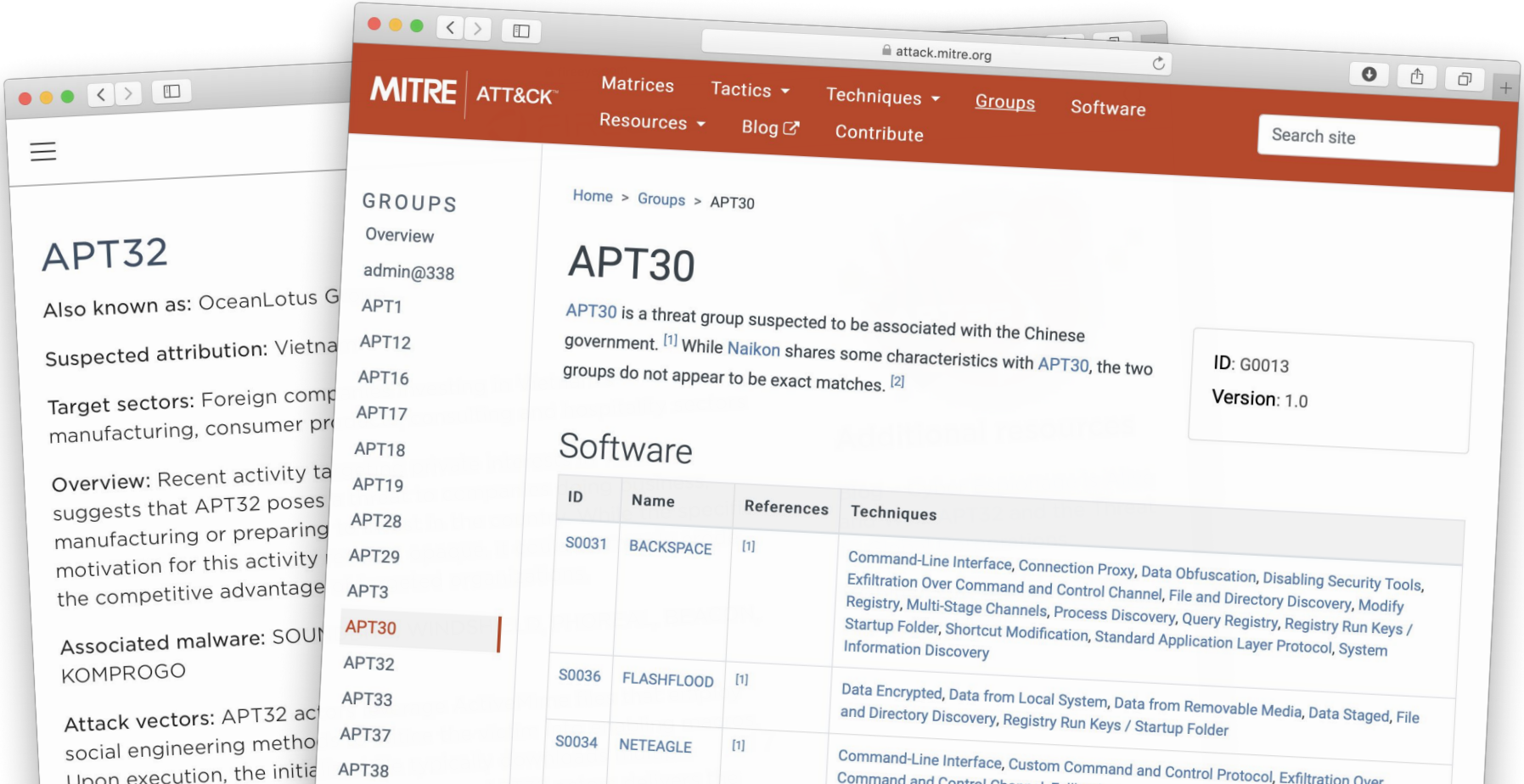
WinXP/7/8/10:
C:\Windows\Prefetch

Interpretation
- Each .pf will include last time of execution, number of times run, and device and file handles used by the program
- Date/Time file by that name and path was first executed
  - Creation Date of .pf file (~10 seconds)
- Date/Time file by that name and path was last executed
  - Embedded last execution time of .pf file
  - Last modification date of .pf file (~10 seconds)
  - Win8-10 will contain last 8 times of execution

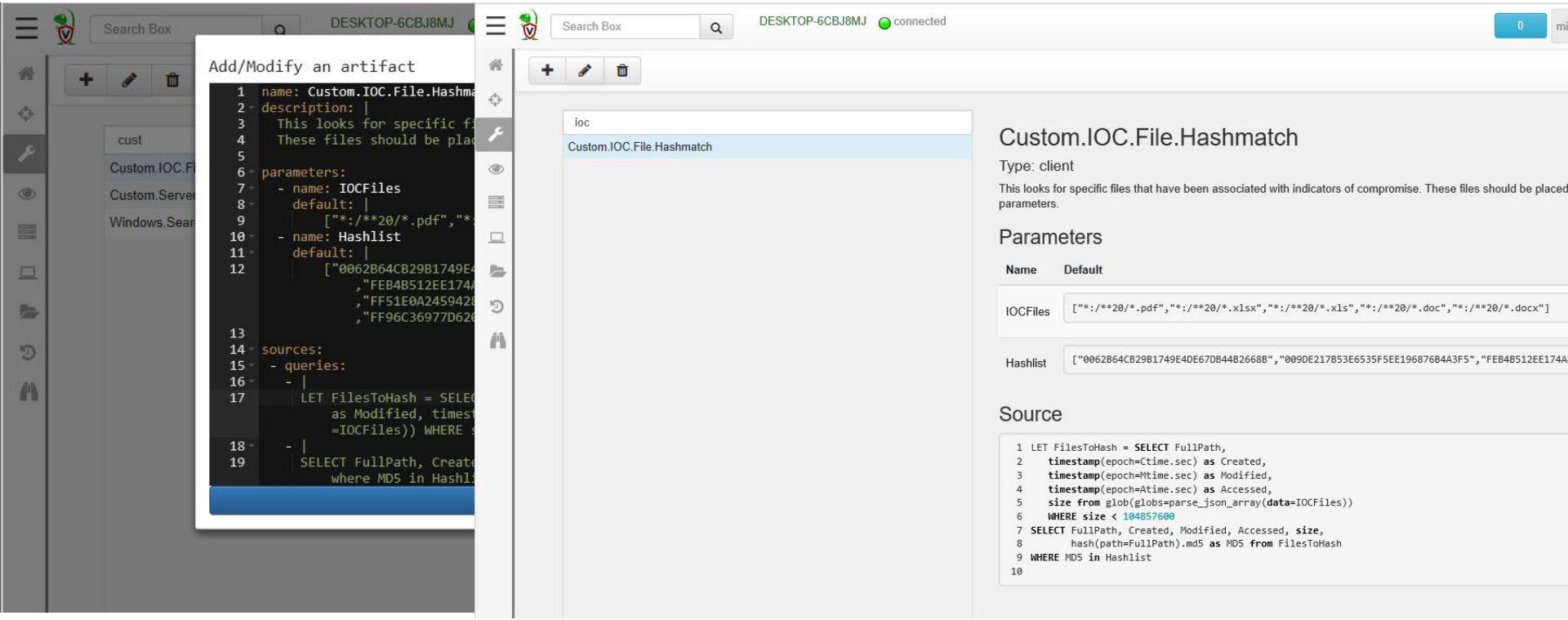
Scenario: Hunt for evidence of program execution



Scenario: Hunt for an APT group using threat intel



Scenario: Hunt for an APT group using threat intel



Scenario: Hunt down “shadow IT”

Dropbox is one common “shadow IT” threat.

It can be accessed through a web browser or an installed program.

Questions we may want to answer from our endpoints:

- Which users have Dropbox accounts?
- Which users have Dropbox installed locally?
- When did they access Dropbox through their web browsers?
- What confidential documents are shared through Dropbox?

Search Box

DESKTOP-6CBJ8MJ connected

0 mic

State	FlowId	Artifacts Collected	Creation Time	Last Active	Creator
✔	F.BKE9AQUGNA20S	Windows.Applications.Chrome.History Windows.Applications.Chrome.Extensions Windows.Applications.Chrome.Cookies	2019-07-03 11:45:47 UTC	2019-07-03 11:45:56 UTC	mic
✔	F.BKE987AQPQP7S	Windows.Applications.Chrome.Extensions	2019-07-03 11:40:13 UTC	2019-07-03 11:40:16 UTC	mic

Artifact Collection | Uploaded Files | Requests | Results | Log | Reports

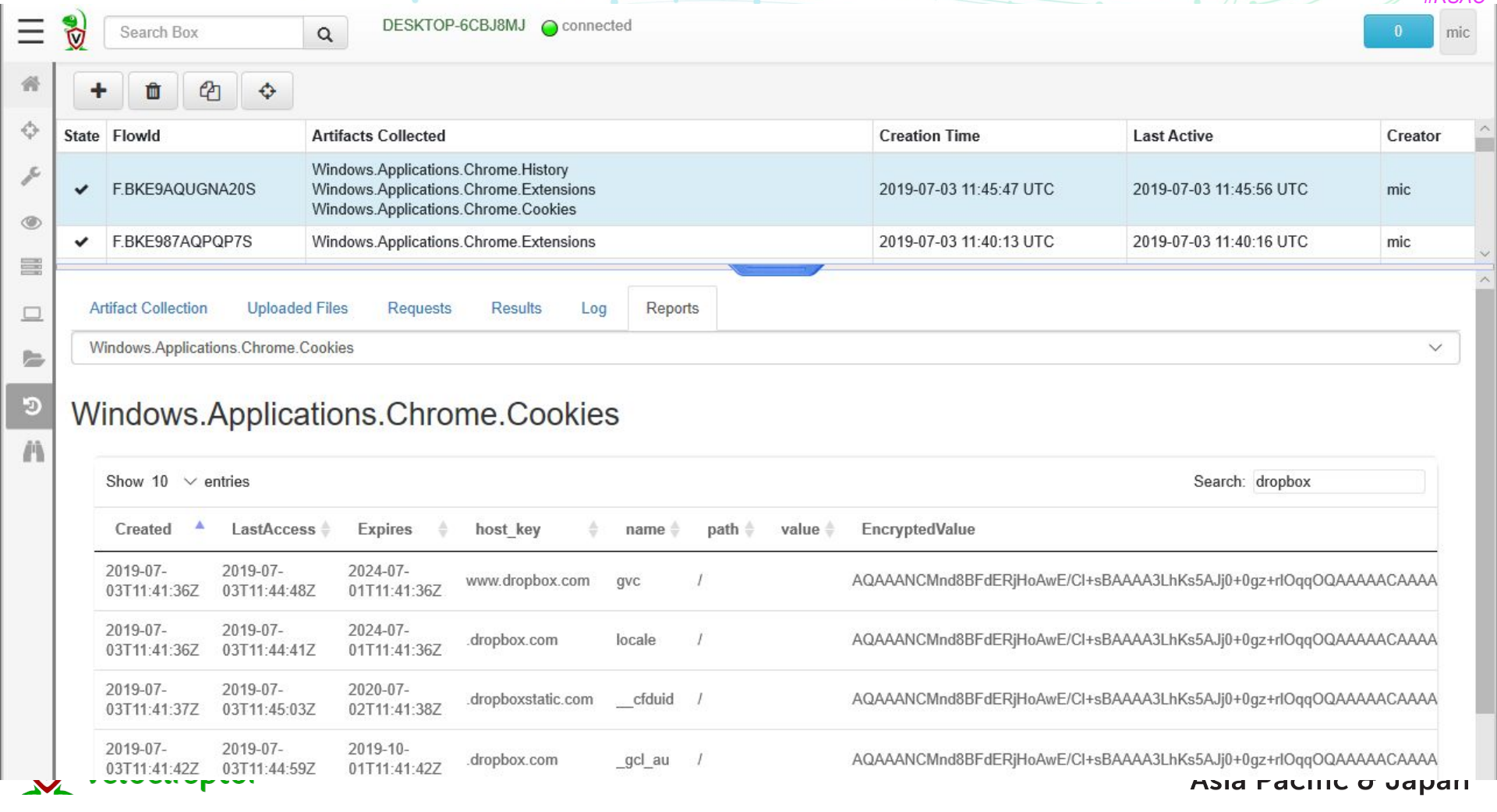
Windows.Applications.Chrome.History

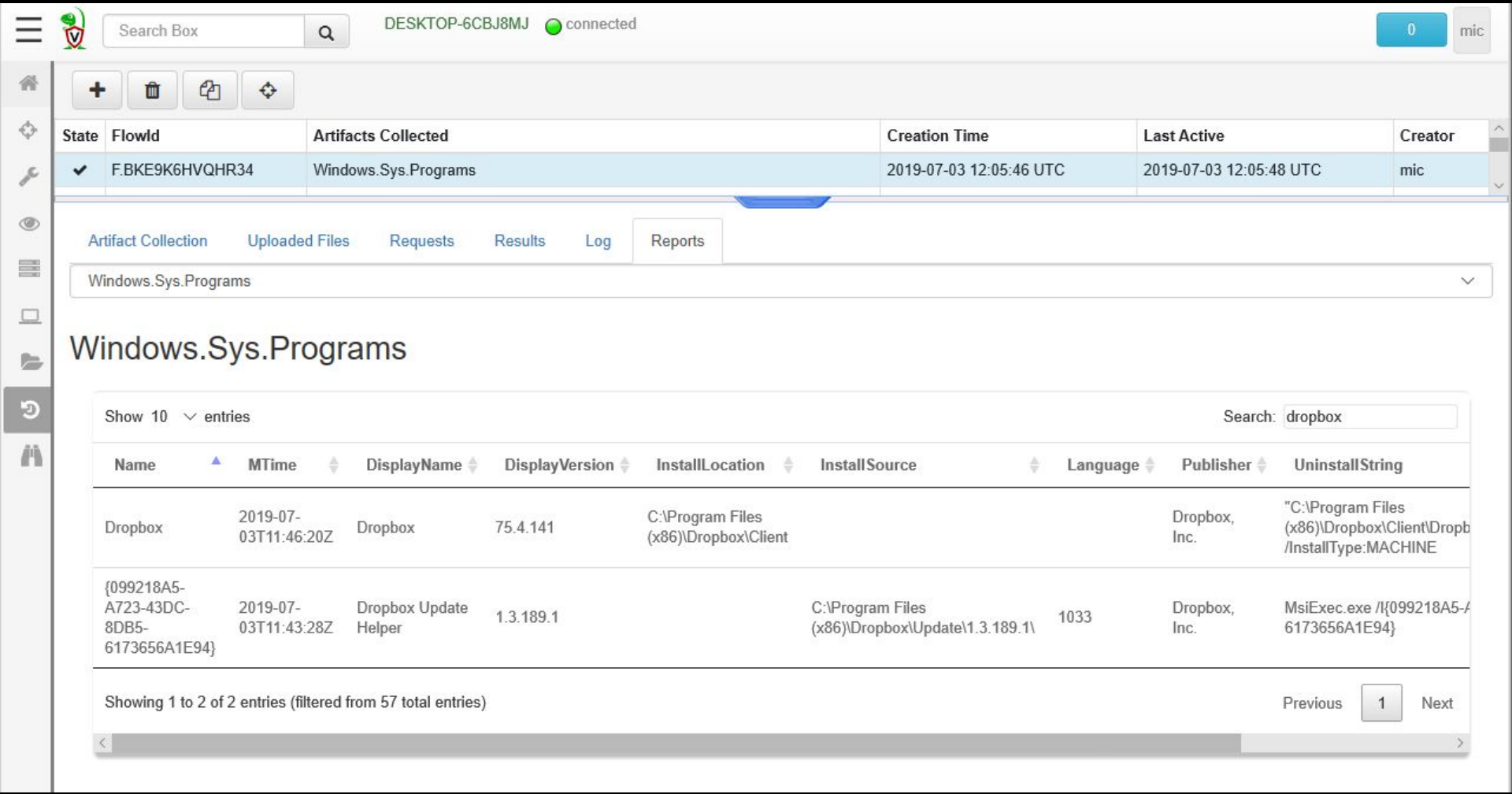
Windows.Applications.Chrome.History

Show 10 entries

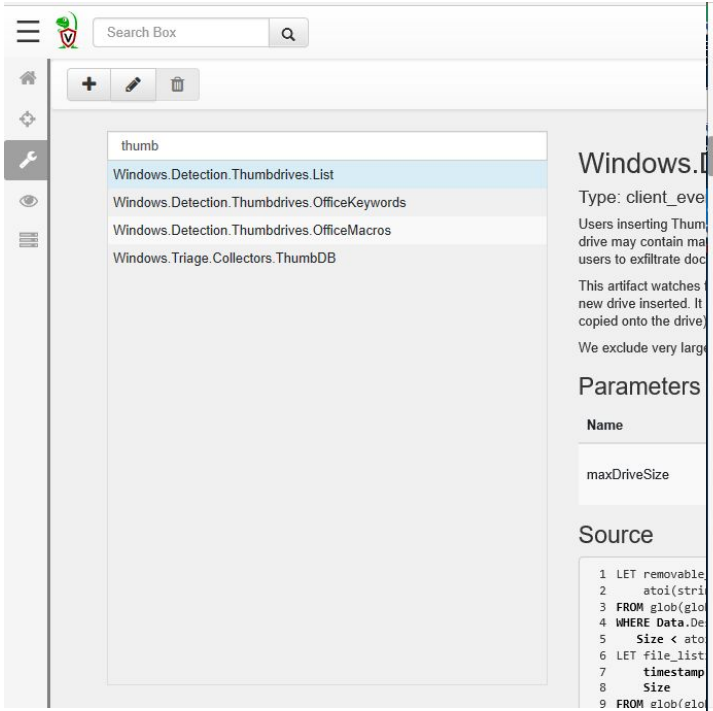
Search: drop

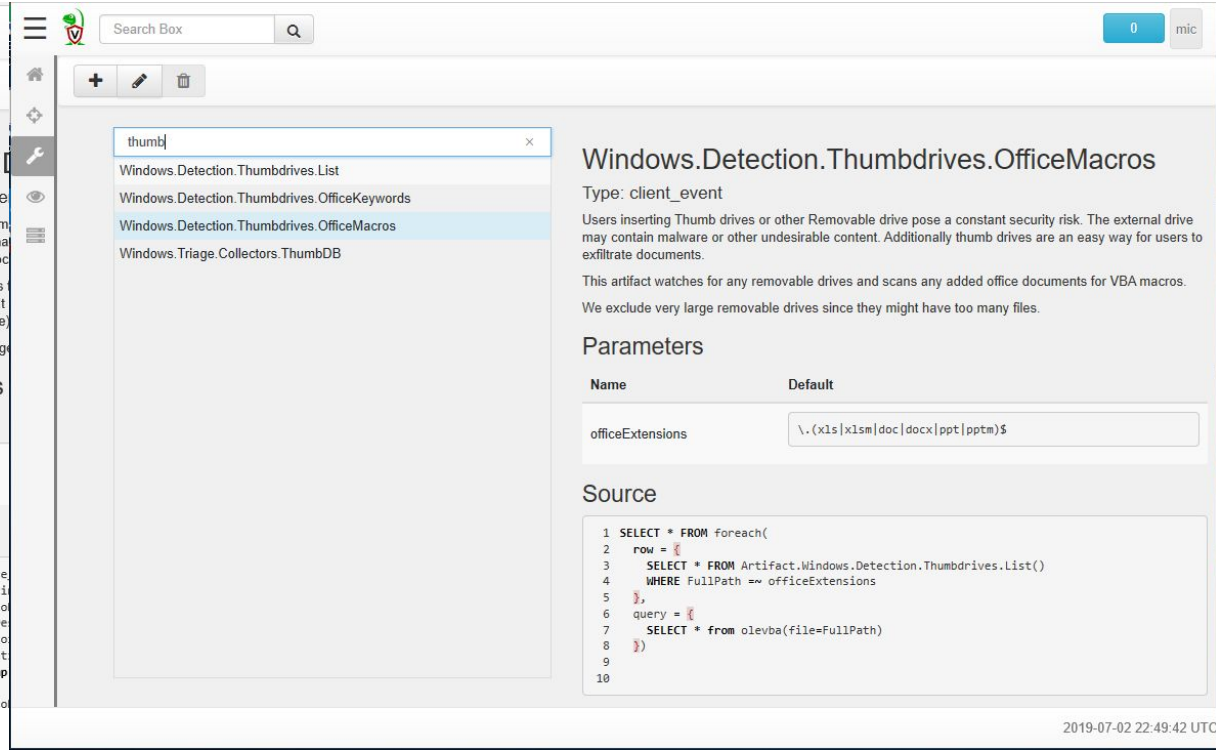
User	FullPath	Mtime	visited_url
test	\C:\Users\test\AppData\Local\Google\Chrome\User Data\Default\History	2019-07-03T11:44:35Z	https://chrome.google.com/webstore/search/dropbox
test	\C:\Users\test\AppData\Local\Google\Chrome\User Data\Default\History	2019-07-03T11:44:35Z	https://www.google.com/search?q=dropbox&rlz=1C1CHBF_enAU843AU843&oq=dropbox&aqs=chrome..69i57j0l5.1871j0j7&sourceid=chrome&ie=U8
test	\C:\Users\test\AppData\Local\Google\Chrome\User Data\Default\History	2019-07-03T11:44:35Z	https://www.dropbox.com/
test	\C:\Users\test\AppData\Local\Google\Chrome\User Data\Default\History	2019-07-03T11:44:35Z	https://www.dropbox.com/individual


Search Box
DESKTOP-6CBJ8MJ
connected
0
mic
State
FlowId
Artifacts Collected
Creation Time
Last Active
Creator
F.BKE9AQUGNA20S
Windows.Applications.Chrome.History
Windows.Applications.Chrome.Extensions
Windows.Applications.Chrome.Cookies
2019-07-03 11:45:47 UTC
2019-07-03 11:45:56 UTC
mic
F.BKE987AQPQP7S
Windows.Applications.Chrome.Extensions
2019-07-03 11:40:13 UTC
2019-07-03 11:40:16 UTC
mic
Artifact Collection
Uploaded Files
Requests
Results
Log
Reports
Windows.Applications.Chrome.Cookies
Windows.Applications.Chrome.Cookies
Show 10 entries
Search: dropbox
Created
LastAccess
Expires
host_key
name
path
value
EncryptedValue
2019-07-03T11:41:36Z
2019-07-03T11:44:48Z
2024-07-01T11:41:36Z
www.dropbox.com
gvc
/
AQAAANCMnd8BFdERjHoAwE/CI+sBAAAA3LhKs5AJj0+0gz+rlOqqOQAAAAACAAA
2019-07-03T11:41:36Z
2019-07-03T11:44:41Z
2024-07-01T11:41:36Z
.dropbox.com
locale
/
AQAAANCMnd8BFdERjHoAwE/CI+sBAAAA3LhKs5AJj0+0gz+rlOqqOQAAAAACAAA
2019-07-03T11:41:37Z
2019-07-03T11:45:03Z
2020-07-02T11:41:38Z
.dropboxstatic.com
__cfduid
/
AQAAANCMnd8BFdERjHoAwE/CI+sBAAAA3LhKs5AJj0+0gz+rlOqqOQAAAAACAAA
2019-07-03T11:41:42Z
2019-07-03T11:44:59Z
2019-10-01T11:41:42Z
.dropbox.com
_gcl_au
/
AQAAANCMnd8BFdERjHoAwE/CI+sBAAAA3LhKs5AJj0+0gz+rlOqqOQAAAAACAAA


Search Box
DESKTOP-6CBJ8MJ
connected
0
mic
State
FlowId
Artifacts Collected
Creation Time
Last Active
Creator
F.BKE9K6HVQHR34
Windows.Sys.Programs
2019-07-03 12:05:46 UTC
2019-07-03 12:05:48 UTC
mic
Artifact Collection
Uploaded Files
Requests
Results
Log
Reports
Windows.Sys.Programs
Windows.Sys.Programs
Show 10 entries
Search: dropbox
Name
MTime
DisplayName
DisplayVersion
InstallLocation
InstallSource
Language
Publisher
UninstallString
Dropbox
2019-07-03T11:46:20Z
Dropbox
75.4.141
C:\Program Files (x86)\Dropbox\Client
Dropbox, Inc.
"C:\Program Files (x86)\Dropbox\Client\Dropb
/InstallType:MACHINE
{099218A5-A723-43DC-8DB5-6173656A1E94}
2019-07-03T11:43:28Z
Dropbox Update Helper
1.3.189.1
C:\Program Files (x86)\Dropbox\Update\1.3.189.1\
1033
Dropbox, Inc.
MsiExec.exe /I{099218A5-A
6173656A1E94}
Showing 1 to 2 of 2 entries (filtered from 57 total entries)
Previous
1
Next

Scenario: Monitor documents on all USB devices





Scenario: Use of Microsoft SysInternal tools

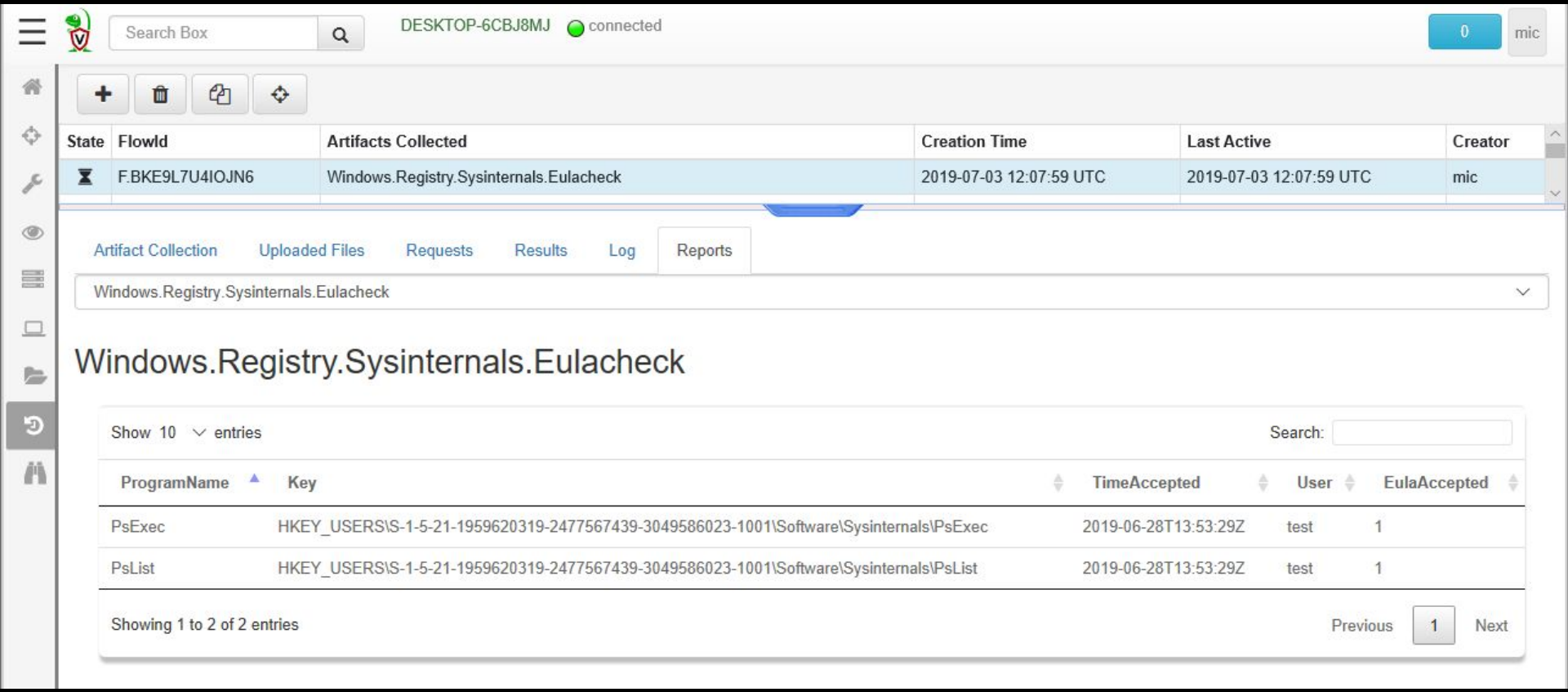
SysInternal tools are powerful system administration tools which are also used by attackers “living off the land”.

Did any SysInternal tools ever run on your endpoint?

For non-administrator accounts, this is very suspicious.

Hint: Sysinternals tools require the user accepting a EULA, which leaves an interesting forensic artifact - a Registry key showing the user accepted the EULA.

We have an artifact for that too!


Search Box
DESKTOP-6CBJ8MJ
connected
0
mic
State
FlowId
Artifacts Collected
Creation Time
Last Active
Creator
F.BKE9L7U4IOJN6
Windows.Registry.Sysinternals.Eulacheck
2019-07-03 12:07:59 UTC
2019-07-03 12:07:59 UTC
mic
Artifact Collection
Uploaded Files
Requests
Results
Log
Reports
Windows.Registry.Sysinternals.Eulacheck
Windows.Registry.Sysinternals.Eulacheck
Show 10 entries
Search:
ProgramName
Key
TimeAccepted
User
EulaAccepted
PsExec
HKEY_USERS\S-1-5-21-1959620319-2477567439-3049586023-1001\Software\Sysinternals\PsExec
2019-06-28T13:53:29Z
test
1
PsList
HKEY_USERS\S-1-5-21-1959620319-2477567439-3049586023-1001\Software\Sysinternals\PsList
2019-06-28T13:53:29Z
test
1
Showing 1 to 2 of 2 entries
Previous
1
Next

Scenario: Monitor all DNS lookups

DNS lookups are an *excellent* network signal.

They can reveal C2 activity and help scope the extent of compromise across a network by showing all clients attempting to connect to known-bad domains.

We can store all DNS lookups from clients, then search this data when threat intel reveals C2 and other suspicious DNS names.

DNS Questions for DESKTOP-6CBJ8MJ

The 1000 most common DNS Queries on this day are listed in the below table. Typically we are looking for two interesting anomalies:

1. Sorting by count for the most frequently called domains. If you do not recognize these it may be possible that a malware is frequently calling out to its C&C.
2. Examining some of the least commonly used DNS names might indicate DNS exfiltration.

Show 10 entries Search:

Total	Name
2	assets.msn.com.
2	ocsp.pki.goog.
2	img-s-msn-com.akamaized.net.
2	about.google.
2	secure-au.imrworldwide.com.
2	www.google.com.
1	googleads.g.doubleclick.net.
1	adservice.google.com.
1	www.google.com.au.
1	sam.msn.com.

Showing 1 to 10 of 30 entries

Velociraptor can hunt for whatever information exists across your endpoints.

So, what do *you* want to find?

Watch this space

Velociraptor is **free and open source** - download and use it today

Ongoing professional development, plus contributions from the DFIR community

Velociraptor is commercially supported through the availability of training and professional services

Development roadmap

More artefacts – based on investigation and other scenarios

More evidence parsers – for more complete forensic analysis

More monitoring functionality – for real-time event detection

Kernel module – for tighter monitoring integration

Wider OS support – more artefacts for OSX and Linux

User interface – more functionality and workflow.

Start hunting today!

Download Velociraptor: github.com/Velocidex/velociraptor

Review the **Quick Start** documentation

Setup a server and deploy some test agents

Start by hunting for some pre-built artefacts

Then customise some hunts to your own requirements

Contribute back with your feedback and ideas

RSAConference2019
Asia Pacific & Japan

Thank you.

https://github.com/Velocidex/velociraptor